STATEMENT OF JAMES L. TAYLOR

DEPUTY INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON MANAGEMENT, INVESTIGATIONS, AND OVERSIGHT

U.S. HOUSE OF REPRESENTATIVES

October 29, 2009

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to appear before you on behalf of the Department of Homeland Security Office of Inspector General. My testimony today will focus on the financial management challenges facing the department and its components, and the progress made so far in addressing these challenges.

Inspectors general are required by law to annually report on the top management challenges for the departments or agencies they oversee. For DHS, the Office of Inspector General has consistently placed financial management high on that list. However, fixing financial management in DHS will require more than just focusing on this one area. Rather, DHS needs to continue its efforts to address its financial management processes, as well as two related areas identified in our November 2008 report: information technology (IT) management and acquisition management. Specifically, DHS must reengineer and standardize its underlying financial processes so they conform to the requirements of the Chief Financial Officer Act of 1990. In addition, DHS must strengthen how it manages information technology, so it is able to develop and implement integrated systems that support redesigned financial processes. Finally, DHS must address longstanding inefficiencies in acquisition management, to ensure it can acquire effectively the information technology needed to meet its financial management responsibilities.

DHS Financial Management

DHS has worked hard to improve financial management, but significant challenges remain. The department consistently has been unable to obtain an unqualified audit opinion, or any audit opinion, on its financial statements. For FY 2008, the independent auditors issued a disclaimer on DHS' financial statements and identified significant deficiencies which were so serious they qualified as material weaknesses. Additionally the OIG issued a disclaimer on DHS' Internal Control Over Financial Reporting (ICOFR). DHS' ability to obtain an unqualified audit opinion, and provide assurances that its system of internal control is designed and operating effectively, is highly dependent upon business process improvements across the department.

Aside from being required by the Chief Financial Officer Act of 1990, financial statement audits provide insight into the status of financial management and progress in resolving weaknesses in processes and systems. For FY 2008, the department was able to reduce the number of conditions leading to the independent auditors' disclaimer of opinion on DHS' financial statements from six to three. As a result, the Office of Financial Management and the Office of Health Affairs no longer contribute to the disclaimer conditions and FEMA remediated all its prior year disclaimer conditions. However, during the FY 2008 audit, new disclaimer conditions were identified at TSA and FEMA. TSA was unable to assert that its capital asset balances were fairly stated and FEMA was unable to assert that its capital asset balances were fairly stated, respectively.

The departmental material weaknesses in internal control were primarily attributable to the Coast Guard, FEMA, and TSA. The Coast Guard's material weaknesses, which have existed since

1994[1], contribute to all six of the department's material weaknesses, while FEMA contributed to four and TSA contributed to three. The Coast Guard also contributes to TSA's financial systems security material weakness due to TSA's reliance on the Coast Guard's financial systems. Although the other components did not have material weaknesses, some had significant deficiencies that, when combined, contributed to the departmental material weaknesses.

DHS' IT Financial Systems

Generally, DHS' IT financial systems are fragmented, do not share data effectively, and over the years have developed security control weaknesses that undermine their overall reliability. Fixing these systems and eliminating security vulnerabilities will be critical to DHS' efforts to improve financial management.

Since 2003, IT general controls have been evaluated as a part of DHS's financial statement audit. This review has included assessing key core financial systems at FEMA, Customs and Border Protection (CBP), TSA, Coast Guard, Federal Law Enforcement Training Center (FLETC), U.S. Immigration and Customs Enforcement, and U.S. Citizenship and Immigration Services. As a part of these reviews, controls over applications being processed on various platforms were evaluated, including Oracle and SAP. The objective of these audits was to evaluate the effectiveness of IT general controls over DHS' financial processing environment and related IT infrastructure as necessary to support the results of the financial statement audit.

We reported in April 2009 that DHS components have taken significant steps to improve financial system security and address prior year IT control weaknesses, which resulted in the closure of more than 40% of our prior year IT control findings.[2] Additionally, some DHS components reduced the severity of the weaknesses when compared to findings reported in the prior year. However, access controls and service continuity continue to be issues at several components including FEMA, Coast Guard and TSA. The most significant weaknesses from a financial statement audit perspective include:

- Excessive unauthorized access to key DHS financial applications;
- Application change control processes that are inappropriate, not fully defined, followed, or effective; and
- Service continuity issues impacting DHS' ability to ensure that DHS financial data is available when needed.

Collectively, the IT control weaknesses we identified limited DHS' ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impacted the internal controls over DHS' financial reporting and its operation, and we consider them to collectively represent a material weakness. The information technology findings were combined into one

[1] DOT-OIG, *Significant Internal Control Weaknesses Identified in Audits of FY 1994 and 1995*, R3-CG-6-011, August 1996.
[2] *Information Technology Management Letter for the FY 2008 DHS Financial Statement Audit(OIG-09-50, April 2009).*

material weakness regarding IT for the FY 2008 audit of the DHS consolidated financial statements.

We recommended that the DHS Chief Information Officer (CIO), in conjunction with the DHS Chief Financial Officer (CFO) and the component CIOs and CFOs make improvements in the areas of access controls, application software development and change controls, service continuity, entity-wide security, system software, and segregation of duties.

Component IT Financial Systems

For FY 2008, we issued separate IT management letter reports for FEMA, CBP, TSA, Coast Guard and FLETC and an overall consolidated IT management letter report that summarized the IT issues for all seven components. Each management letter addressed the IT security issues at each component and provided individual component level findings and recommendations. In each of these management letters we recommended that the component CIOs and CFOs in conjunction with the DHS CIO and CFO work to address the issues noted in our reports.

Coast Guard

We reported in March 2009 that the Coast Guard took corrective action to address nearly half of its prior year IT control weaknesses.[3] However, we continued to identify IT general control weaknesses. The most significant weaknesses from a financial statement audit perspective related to the development, implementation, and tracking of financial systems coding changes, and the design and implementation of configuration management policies and procedures.

Of the 22 findings identified during FY 2008 testing, 21 were repeat findings, either partially or in whole from the prior year, and 1 was a new IT finding. These findings represent weakness in four of the six key control areas. The areas impacted included Application Software Development and Change Controls, Access Controls, Service Continuity, and Entity-Wide Security Program Planning and Management. The majority of the findings were inherited from the lack of properly designed, detailed, and consistent guidance over financial system controls.

Specifically, the findings stem from 1) unverified access controls through the lack of user access privilege re-certifications, 2) entity-wide security program issues involving civilian and contractor background investigation weaknesses, 3) inadequately designed and operating change control policies and procedures, 4) patch and configuration management weaknesses within the system, and 5) the lack of updated disaster recovery plans which reflect the current environment identified through testing. These weaknesses may increase the risk that the confidentiality, integrity, and availability of system controls and Coast Guard financial data could be exploited thereby compromising the integrity of financial data used by management and reported in the DHS financial statements.

[3] *Information Technology Management Letter for the United States Coast Guard Component of the FY 2008 DHS Financial Statement Audit (OIG-09-47, March 2009).*

CBP

We reported in April 2009 that CBP took corrective action to address prior year IT control weaknesses.[4] For example, CBP made improvements in how it tracks the hiring, termination and systems access of contracted employees within the Office of Information Technology (OIT). However, during FY 2008, identify IT general control weaknesses continued to exist at CBP. The most significant weaknesses, from a financial statement audit perspective, related to controls over access to programs and data.

Although improvement was noted in the audit, many of the conditions identified at CBP in FY 2007 have not been corrected because CBP still faces challenges related to the merging of numerous IT functions, controls, processes, and organizational resource shortages. During FY 2008, CBP took steps to address these conditions. Despite these improvements, CBP needs further stress on the monitoring and enforcement of access controls. CBP needs to further emphasize the importance of developing and implementing well-documented procedures at the system and entity-level.

FEMA

FEMA took corrective action to address prior year IT control weaknesses. We reported in March 2009 that FEMA made improvements by restricting access to offline account tables, implementing an alternate processing site for one of its financial applications, and improving the process for retaining National Flood Insurance Program (NFIP) change control documentation.[5] However, during FY 2008, IT general control weaknesses at FEMA still existed. The most significant weaknesses from a financial statement audit perspective related to controls over access to programs and data and controls over program changes.

Of the 26 findings identified during the FY 2008 testing, 15 were repeat findings, either partially or in whole from the prior year, and 11 were new findings. These findings were representative of five of the six key control areas. Specifically, the findings stem from: 1) inadequately designed and operating access control policies and procedures relating to the granting of access to systems and supervisor re-certifications of user access privileges, 2) lack of properly monitored audit logs, 3) inadequately designed and operating change control policies and procedures, 4) patch and configuration management weaknesses within the system, and 5) the lack of tested contingency plans. These weaknesses may increase the risk that the confidentiality, integrity, and availability of system controls and FEMA financial data could be exploited, thereby compromising the integrity of financial data used by management and reported in the DHS financial statements.

[4] *Information Technology Management Letter for the FY 2008 Customs and Border Protection Financial Statement Audit (OIG-09-59, April 2009).*

[5] *Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2008 DHS Financial Statement Audit (OIG-09-48, March 2009).*

FLETC

We reported in April 2009 that FLETC made minimal progress on its control weaknesses.[6] Therefore, many of the prior year Findings and Recommendations (NFR) could not be closed completely due to the reliance on the impending Momentum application upgrade, the decommissioning of Procurement Desktop and the installation of new hardware that would improve the overall IT security structure at FLETC. As a result, there was one (1) prior year NFR closed, twenty (27) reissued NFRs, and three (3) new NFRs issued to FLETC.

The IT testing at FLETC disclosed matters involving the internal controls over financial reporting and its operation that we consider to be a significant deficiency under AICPA standards. Deficiencies in the design and operation of FLETC's internal controls which could adversely affect the agency's financial statements were noted. Deficiencies also existed in entity-wide security planning, access controls, application development and change control, system software, segregation of duties, and service continuity that have contributed to the significant deficiency.

TSA

In FY 2008, TSA took corrective action to address prior year IT control weaknesses. We reported in April 2009 that TSA made improvements in testing disaster recovery procedures, reviewing audit logs, and implementing emergency response training for all personnel with data center access.[7] However, IT general control weaknesses that impact TSA's financial data remain. The most significant weaknesses from a financial statement audit perspective related to controls over the termination of the contract with the software support vendor, the design and implementation of configuration management policies and procedures, and the development, implementation, and tracking of coding changes to the software maintained for TSA by the Coast Guard.

Of the 15 findings identified during our FY 2008 testing, 13 are repeat findings, either partially or in whole from the prior year, and 2 are new IT findings. These findings represent weaknesses in four of the six key control areas. Specifically, 1) unverified access controls through the lack of comprehensive user access privilege re-certifications, 2) entity-wide security program issues involving civilian and contractor background investigation weaknesses, 3) inadequately designed and operating change control policies and procedures, and 4) the lack of updated disaster recovery plans which reflect the current environment identified through testing. These weaknesses may increase the risk that the confidentiality, integrity, and availability of system controls and TSA financial data could be exploited thereby compromising the integrity of financial data used by management and reported in TSA's financial statements.

[6] *Information Technology Management Letter for the Federal Law Enforcement Training Center FY 2008 Financial Statement Audit (OIG-09-63, April 2009).*

[7] *Information Technology Management Letter for the Transportation Security Administration FY 2008 Financial Statement Audit (OIG-09-62, April 2009).*

DHS IT Disaster Recovery Efforts

Following a service disruption or a disaster, DHS must be able to recover its IT systems quickly and effectively in order to continue essential functions, including financial management support. In May 2005, we reported on deficiencies in the Department of Homeland Security's disaster recovery planning for information systems.[8] We recommended that the department allocate the funds needed to implement an enterprise-wide disaster recovery program for mission critical systems, require that disaster recovery capabilities be included in the implementation of new systems, and ensure that disaster recovery-related documentation for mission critical systems be completed and conform to current government standards.

We conducted a follow-up audit last year and reported in April 2009 that the department has made progress in establishing an enterprise-wide disaster recovery program.[9] Specifically, the department has allocated funds for this program since fiscal year 2005, and by August 2008 had established two new data centers. Further, the department now includes contingency planning as part of the system authorization process and it has issued guidance to ensure that contingency planning documentation conforms to government standards.

While the department has strengthened its disaster recovery planning, more work is needed. For example, the two new data centers need interconnecting circuits and redundant hardware to establish an active-active processing capability.
We noted that not all critical departmental information systems have an alternate processing site. Further, disaster recovery guidance does not conform fully to government standards. Finally, risk assessments of the data centers are outdated.

In our FY 2008 report, we recommended that the Chief Information Officer implement the necessary circuits and redundant resources at the new data centers; ensure that critical departmental information systems have complete contingency planning documentation; and conform departmental contingency planning guidance to government standards. Additionally, the department should reassess data center risks whenever significant changes to the system configuration have been made.

The FY 2008 financial statement audit noted that service continuity issues continue to impact DHS' ability to ensure that DHS financial data is available when needed, including instances where the Continuity of Operations Plan (COOP) does not include an accurate listing of critical information technology systems, did not have critical data files and an alternate processing facility documented, and was not adequately tested, and various weaknesses identified in alternate processing sites. Service continuity is one of the main IT general control areas that continue to present a risk to financial systems data integrity for DHS' financial systems.

Among recommendations for service continuity for DHS' financial systems were to update the COOP to document and prioritize an accurate listing of critical IT systems, ensure that alternate processing sites are made operational, and test backups at least quarterly.

---

[8] *Disaster Recovery Planning for DHS Information Systems Needs Improvement (OIG-05-22, May 2005).*
[9] *DHS' Progress in Disaster Recovery Planning for Information Systems* (OIG-09-60, April 2009).

Transformation and Systems Consolidation (TASC)

DHS has recognized that it needs to improve its financial management processes, as well as the systems that support those processes. Toward that end, DHS is moving ahead with TASC, an enterprise-wide initiative, aimed at modernizing, transforming, and integrating the financial, acquisition, and asset management capabilities of DHS components. According to DHS, TASC is not an update of legacy systems, but an implementation of integrated financial, asset and procurement management capabilities that will subsume many systems and standardize business processes. The resulting system, once implemented, is aimed at providing a real-time (providing immediate viewing of data), web-based system (accessed from anywhere) of integrated business processes that will be used by component financial managers, service providers, program managers, and auditors to make sound business decisions to support the DHS mission.

The goals and objectives of the TASC initiative are numerous and reflect the collective input from the components. TASC also represents an effort to leverage the work done by Office of Federal Financial Management (OFFM) and will achieve full compliance with the rigid standards outlined by OFFM. TASC will implement enhanced capabilities to achieve the following goals:

- Create end to end standardized integrated business processes
- Support timely financial management
- Enable the acquisition of best value goods and services that meet the department's quality and timeliness requirements
- Enable consolidated asset management across all components
- Create a standard central accounting line

TASC is DHS' third attempt to address comprehensively its longstanding financial management process and system problems. The first effort, known as the Electronically Managing Enterprise resources for Government Effectiveness and Efficiency (e-Merge) project, was canceled in December 2005 after DHS had spent $24 million on what DHS officials had determined to be a failure. The second effort focused on moving DHS components to one of two financial systems platforms: SAP and Oracle. However, a federal court ruled in *Savantage Financial Services, Inc. vs. United State* that DHS' decision to use Oracle and SAP financial software systems via "Brand Name Justification" document is improper sole source procurement in violation of the Competition in Contracting Act. In response to this decision, RMTO revised its financial systems consolidation strategy to the current approach.

TASC is a high risk initiative that will take years to complete, potentially costing over $1 billion. We are presently completing a review of DHS' efforts in planning and implementing TASC, and plan to report on the results of our review in a few months.

In summary, the DHS CFO and CIO in conjunction with the component CFOs and CIOs are responsible for working together to standardize DHS' core financial systems. However, weaknesses in financial management processes and IT security controls over these systems continue to hinder the department's ability to effectively produce accurate consolidated financial

information. DHS is currently in the processes of developing and implementing a new financial system solution that will modernize, transform and integrate financial, acquisition, and asset management information for DHS components. Once DHS addresses the current issues in financial processing and IT security controls and successfully develops and implements a new financial systems solution, the department will be able to promote overall efficiency and effectiveness in its financial management.

Mr. Chairman, this concludes my prepared statement. Thank you for this opportunity and I welcome any questions from you or Members of the Subcommittee.